UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/574,630	05/12/2008	Ernst Haselsteiner	AT03 0055 US1	1877

65913 7590 11/24/2008

NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	PAPER NUMBER
2431	
NOTIFICATION DATE	DELIVERY MODE
11/24/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	**Application No.** 10/574,630	**Applicant(s)** HASELSTEINER ET AL.
	Examiner KAVEH ABRISHAMKAR	**Art Unit** 2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 April 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *4/04/2006*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on April 4, 2006. Claims 1-15 were originally received for consideration. Per the received preliminary amendment, claims 1-15 are currently amended.

2. Claims 1-15 are presently pending consideration.

Information Disclosure Statement

3. An initialed and dated copy of Applicant's IDS form 1449, received on 4/04/2006, is attached to this Office action.

Claim Objections

4. Claim 6 is objected to because of the following informalities: The word “carrier" is misspelled "carner." Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-15 are rejected under 35 U.S.C. 102(a) as being anticipated by Proudler et al. (EP 1280042 A2).

Regarding claim 1, Proudler discloses:

A method of identifying and/or verifying hardware and/or software of an appliance and of a data carrier which is provided to cooperate with the appliance, comprising the following steps:

transmitting first authorization data of the hardware and/or software to a first unit (paragraph 0016-0019, 0029-0030, 0041, 0049-0051: *sends a nonce to the trusted device, and receives a response used to verify the trusted device*);

comparing the first authorization data of the hardware and/or software that has been transmitted to the first unit with first verification data stored in the first unit (paragraph 0016: *identity and integrity metric are compared with expected values provided by a trusted party*)

authorizing the hardware and/or software once it has been ascertained that there is coincidence between the first authorization data provided by the hardware and/or software and the first verification data stored in the first unit (paragraph 0016: *identity and integrity metric are compared with expected values provided by a trusted party, and if there is a match, the device is trusted*)

transmitting second authorization data of a data carrier to a second unit (paragraph 0022, 0029, 0044: *verification between a smart card and a trusted device*);

comparing the second authorization data in the second unit with second verification data stored in the second unit (paragraph 0022, 0029, 0044: *verification between a smart card and a trusted device*)

authorizing the data carrier if there is coincidence between the second authorization data and the second verification data stored in the second unit (paragraph 0022, 0029, 0044: *verification between a smart card and a trusted device*)

wherein a direct data exchange is carried out between the first unit and the second unit (paragraph 0041, 0052: *communication between the trusted device and the platform after logical binding*).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Proudler discloses:

A method as claimed in claim 1, wherein the direct data exchange between the first unit and the second unit comprises a transmission of encrypted data and a comparison and/or decryption of data transmitted between the first unit and the second unit (paragraph 0019, paragraph 0051: cryptographic processes).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Proudler discloses:

A method as claimed in claim 1, wherein the data exchange between the first unit and the second unit is carried out prior to an identification and/or verification of first authorization data of the hardware and/or software and of second authorization data of the data carrier (paragraph 0041, 0052: *communication between the trusted device and the platform after logical binding*).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Proudler discloses:

A method as claimed in claim 1, wherein a central arithmetic unit of the first unit and a central arithmetic unit of the second unit jointly access at least one ROM memory one RAM memory and/or one non-volatile memory (paragraph 0030-0034: *measurement function has access to non-volatile memory and volatile memory to access the stored hash program, private key, and the acquired integrity metric in the form of a digest*).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Proudler discloses:

A method as claimed in claim 1, wherein encryption of the first authorization data and of the second authorization data is carried out in the first unit and in the second unit (paragraph 0019, paragraph 0051: *cryptographic processes*).

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Proudler discloses:

A method as claimed in claim 1, wherein the second authorization data are obtained from a smartcard or a tag or a label that forms the data carner (paragraph 0022, 0029, 0044: *verification between a smart card and a trusted device*).

Regarding claim 7, Proudler discloses:

A circuit for identifying and/or verifying hardware and/or software of an appliance and of a data carrier which is provided to cooperate with the appliance, comprising:

a first unit for identifying and/or verifying the hardware and/or software of the appliance (paragraph 0016-0019, 0029-0030, 0041, 0049-0051: *sends a nonce to the trusted device, and receives a response used to verify the trusted device*), comprising a central arithmetic unit and at least one memory and an interface to the hardware and/or software that is to be identified and/or verified (paragraph 0030-0034: *measurement function has access to non-volatile memory and volatile memory to access the stored hash program, private key, and the acquired integrity metric in the form of a digest*), and

a second unit comprising a central arithmetic unit and at least one memory and an interface to an external data carrier and also an interface to the hardware and/or software (paragraph 0022, 0029, 0044: *verification between a smart card and a trusted device*),

wherein a communication interface is provided between the central arithmetic units of the first unit and the second unit (paragraph 0041: *communication between platforms*).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Proudler discloses:

A circuit as claimed in claim 7, wherein the memories of the first unit and of the second unit are formed by a ROM memory and a RAM memory and/or a non-volatile memory (paragraph 0030-0034: *measurement function has access to non-volatile memory and volatile memory to access the stored hash program, private key, and the acquired integrity metric in the form of a digest*).

Claim 9 is rejected as applied above in rejecting claim 7. Furthermore, Proudler discloses:

A circuit as claimed in claim 7, wherein the ROM memories and/or the RAM memories and/or the non-volatile memories of the first unit and of the second unit are in each case combined to form a common ROM memory and/or a common RAM memory and/or a common non-volatile memory (paragraph 0030-0034: *measurement function has access to non-volatile memory and volatile memory to access the stored hash program, private key, and the acquired integrity metric in the form of a digest*).

Claim 10 is rejected as applied above in rejecting claim 7. Furthermore, Proudler discloses:

A circuit as claimed in claim 7, wherein the first unit and the second unit in each case comprise an encryption device (paragraph 0019, paragraph 0051: *cryptographic processes*).

Claim 11 is rejected as applied above in rejecting claim 7. Furthermore, Proudler discloses:

A circuit as claimed in claim 7, wherein the central arithmetic unit of the first unit and the central arithmetic unit of the second unit are combined to form a common central arithmetic unit which common central arithmetic unit has the integrated communication interface, and wherein the common central arithmetic unit is connected by an interface to the hardware and/or software that is to be identified and/or verified (paragraph 0030-0034: *measurement function has access to non-volatile memory and volatile memory to access the stored hash program, private key, and the acquired integrity metric in the form of a digest*).

Claim 12 is rejected as applied above in rejecting claim 7. Furthermore, Proudler discloses:

A circuit as claimed in claim 7, wherein the interface to the external data carrier is designed for contactless communication with the external data carrier (paragraph 0022, 0029, 0044: *verification between a smart card and a trusted device*).

Claim 13 is rejected as applied above in rejecting claim 14. Furthermore, Proudler discloses:

A circuit as claimed in claim 7, wherein the external data carrier is formed by a smartcard or a tag or a label (paragraphs 0032-0034: *label or a smart card*).

Claim 14 is rejected as applied above in rejecting claim 7. Furthermore, Proudler discloses:

An appliance which comprises as hardware at least one central arithmetic unit which central arithmetic unit is designed to run software and to obtain data from an external data carrier cooperating with the appliance, wherein a circuit as claimed in claim 7 is coupled to the central arithmetic unit (paragraph 0022, 0029, 0044: *verification between a smart card and a trusted device*).

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Proudler discloses:

An appliance as claimed in claim 14, wherein the central arithmetic unit of the appliance is coupled via an interface integrated in the central arithmetic unit of the appliance to the circuit integrated in the central arithmetic unit (paragraph 0030-0034).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Examiner, Art Unit 2431

/K. A./
11/19/2008
Examiner, Art Unit 2431